UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,058	07/21/2000	David W. Carman	NAIIP080/99.123.01	4463

28875 7590 02/27/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	9

DATE MAILED: 02/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,058	CARMAN ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1-15 are rejected under 35 U.S.C. 102(a) as being anticipated by Balenson et al.

In reference to claim 1:

Balenson et al. (Page 22, Figure 6) discloses an authentication method, comprising:

Generating a plurality of authentication tags for a message, each of said plurality of authentication tags reflecting a different authentication strength, where the plurality of tags are subset tags which can be used as different gears that represent the levels of authentication strength one wishes to use.

Transmitting said plurality of authentication tags in association with said message to at least one receiver, where the one receiver can decide whether to verify the message using *whole_tag* or only verify the subset of a message that contributed to a *subset_tag* computation. (page 22, 2nd paragraph)

In reference to claim 2:

Balenson et al. (page 19, Figure 4) discloses a method wherein one of said plurality of authentication tags is generated using a hash-based message authentication code algorithm, denoted by the HMAC.

In reference to claim 4:

Balenson et al. (page 22, 2nd paragraph) discloses a method wherein one of said plurality of authentication tags is generated using a partial message authentication code algorithm, where only part of a message is used to generate the MAC subset_tag.

In reference to claim 5:

Balenson et al. (page 22) discloses a method wherein

- two or more of said plurality of authentication tags are generated using a nested structure that includes a plurality of inner functions that are each operative on a particular collection of message parts to produce a plurality of intermediate hash results,
    - wherein a plurality of distinct combinations of one or more of said plurality of intermediate hash results are used by an outer hash function to produce said two or more authentication tags, where the authentication tags are the subset_tags or the whole_tag.

In reference to claim 6:

Balenson et al. (page 22, paragraph 1) discloses a method wherein said plurality of authentication tags are appended to said messages, where the plurality of tags includes the created subset_tags.

In reference to claim 7:

Balenson et al. (page 22) discloses an authentication method, comprising:

- Generating a plurality of collections of parts of said message, where the collection of parts are words of the messages.
- Processing each of said plurality of collections of message parts using a respective inner hash function to produce a plurality of intermediate hash results, where each collection of words goes to a specific hash function shown in figure 6.
- Processing a plurality of distinct combinations of said plurality of intermediate hash results using an outer hash function to produce a plurality of authentication tags, where the plurality of authentication tags are the subset_tags and the whole_tag.
- Transmitting said plurality of authentication tags in association with said message to at least one receiver, where it is disclosed that the authentication tags are associated with each message (paragraph 1)

In reference to claim 8:

Balenson et al. (page 22, Fig 5.) discloses a method wherein said plurality of collection of parts of said message are distinct, where the collection of parts are distinct in that each collection of parts is divided between the inner functions.

In reference to claim 9:

Balenson et al. (page 22) discloses a method wherein a collection of parts of said message is a collection of bits, where each message part is understood to be a word, which is a collection of bits.

In reference to claim 10:

Balenson et al. (page 22) discloses a method wherein a single inner hash function is used to create said plurality of intermediate hash results, where the plurality of intermediate hash results comes out from either the intermediate values in the computation of the inner MAC function, processing the collection of message blocks, or the each intermediate result produced in (page 21, Fig 5)

In reference to claim 11:

Balenson et al. (page 22, Figure 6) discloses a method wherein two inner functions are used to produce:

- a first and a second intermediate hash result, wherein said first intermediate hash result is processed using an outer function to produce a first authentication tag (subset_tag1)
- said second intermediate hash result is processed using said outer function to produce a second authentication tag. (subset_tag2)
- and said first and second intermediate hash results are processed using said outer function to produce a third authentication tag. (whole_tag)

In reference to claim 12:

Balenson et al. (page 22) discloses an authentication method, comprising:

- Receiving a plurality of authentication tags, where (Figure 6) discloses a message that is sent to the receiver consisting of three authentication tags.
- Selecting one of said plurality of authentication tags, where either one of the subset_tags are selected or the whole_tag is selected. (2nd paragraph)
- Authenticating a message associated with said plurality of authentication tags using said selected authentication tag, where the authentication tag selected is used for authentication.

In reference to claim 13:

Balenson et al. (page 22) discloses a method wherein an authentication tag is selected based upon a desired authentication strength, where if the whole_tag is selected, a greater authentication strength is desired, while if subset_tags are used, the authentication would less secure, but faster.

In reference to claim 14:

Balenson et al. (page 22) discloses a method wherein an authentication tag is selected based upon a performance level.

In reference to claim 15:

Balenson et al. (page 17, figure 3) discloses a method wherein an authentication tag is selected based on a processor load.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balenson et al. and Black et al.

In reference to claim 3:

Balenson et al. discloses all of claim 3 except a method wherein one of said plurality of authentication tags is generated using a universal message authentication code algorithm.

Black et al. discloses the UMAC algorithm used for message authentication codes. Black et al. (Section 1, Introduction) teaches UMAC has been designed extreme speed and provable security in mind. The speed of UMAC is much faster than HMAC-SHA-1 and faster than MMH by a large margin.

It would have been obvious for one of ordinary skill in the art at the time of invention to apply the UMAC algorithm to the ACSA system given, it's specific design for extreme performance while retaining provable security. Furthermore, because the objective of the ACSA system was to optimize the speed of the algorithm used in the inner function of its NMACs, UMAC would fit perfectly as a candidate function described in Balenson et al. (page 20, paragraphs 4 & 5)

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

February 12th 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100